MILLER CANFIELD

POLISH LAW REVIEW
*PRZEGLĄD PRAWA POLSKIEGO* **NR 2/2017**

Poland USA Canada Mexico China

*Z przyjemnością informujemy, że w tym roku mija **25 lat** od rozpoczęcia w Polsce działalności przez Kancelarię Adwokatów i Radców Prawnych Miller Canfield. Serdecznie dziękujemy wszystkim naszym Klientom za zaufanie, jakim nas obdarzyli.*

***

*It is our great pleasure to inform you that this year marks the **25th anniversary** since the Law offices of Miller Canfield became established in Poland. We would like to take this opportunity to express our heartfelt thanks to our Clients for the unwavering confidence and trust.*



## WSTĘP

17 maja 2016 roku weszło w życie Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Zacznie ono bezpośrednio obowiązywać w krajowych porządkach prawnych od dnia 25 maja 2018 roku.

Ogólne Rozporządzenie o Ochronie Danych, zwane także „RODO" lub „GDPR" (dalej w niniejszej publikacji, jako **„Rozporządzenie"** lub **„RODO"**), stanowi kompleksową regulację dotyczącą zakresu obowiązków podmiotów, które przetwarzają dane osobowe, a jego celem jest stworzenie nowej perspektywy dla ochrony danych osobowych. Wiąże ono wszystkie podmioty, które przetwarzają dane osobowe w związku z prowadzoną działalnością gospodarczą. Uregulowanie zasad ochrony danych osobowych rozporządzeniem, a nie jak to miało miejsce poprzednio – dyrektywą, ma na celu ujednolicenie przepisów na obszarze całej Unii Europejskiej. Jednolita regulacja ma ułatwić prowadzenie transgranicznej działalności

## INTRODUCTION

On 17 May 2016, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC came into force. It is set to become directly applicable as part of national legislation as of 25 May, 2018.

The General Data Protection Regulation also known as the "GDPR" (hereinafter in this edition of the Polish Law Review as **"Regulation"** or **"GDPR"**) is a comprehensive legislative act relating to the scope of obligations of personal data processors and its aim is to develop a new perspective on personal data protection. It binds upon all the processors processing personal data in connection with their business activity. The aim of laying down the rules of data protection in a regulation, rather than in a directive (as it was previously), is to harmonise those provisions throughout the European Union. Uniform regulation is to facilitate cross-border business activity. Discrepancies in the data protection laws between different Member States

gospodarczej. Zmniejszeniu ulegną rozbieżności w prawie ochrony danych osobowych występujące w poszczególnych krajach Unii Europejskiej, a tym samym przedsiębiorcy z większą pewnością będą mogli stosować mechanizmy ochrony danych osobowych we wszystkich krajach Unii Europejskiej, w których prowadzą swoją działalność. Nie oznacza to jednak, że Rozporządzenie całkowicie zastąpi krajową Ustawę o ochronie danych osobowych. Ustawa stanowić będzie uzupełnienie przepisów Rozporządzenia. W praktyce przedsiębiorcy przetwarzający dane osobowe będą weryfikowali zgodność swoich działań, odwołując się wprost do przepisów Rozporządzenia, oraz uzupełniając je zapisami znowelizowanej Ustawy o ochronie danych osobowych.

of the European Union will be reduced, as a result of which enterprises will be more confident when applying the personal data protection mechanisms in all the Member States of the European Union in which they operate. However, it does not mean that the Regulation will completely replace the national Act on Personal Data Protection. The Act will be supplementing the provisions of the Regulation. In practice, enterprises processing personal data will verify compliance of their activities by referring directly to the provisions of the Regulation and supplementing them with the provisions of the amended Act on Personal Data Protection.

Na mocy Rozporządzenia utworzona została Europejska Rada Ochrony Danych („EROD"), która przejęła dotychczasowe obowiązki Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych. EROD jest organem Unii Europejskiej, który posiada osobowość prawną i działa w sposób niezależny. Jego zadaniem jest zapewnienie spójnego stosowania przepisów Rozporządzenia. Na poziomie krajowym zaś przestrzeganie nowych przepisów monitorować będą organy nadzoru. Nowe przepisy wprowadzają zasadę one-stop shop, która oznacza, że, w przypadku, gdy przedsiębiorca przetwarza dane osobowe w więcej niż jednym państwie członkowskim, to organ nadzoru właściwy dla głównej siedziby przedsiębiorcy będzie właściwy także względem transgranicznego przetwarzania danych, jak również wszystkich obowiązków tego podmiotu z zakresu realizacji zapisów Rozporządzenia. Organy nadzoru poszczególnych państw członkowskich pozostaną nadal właściwe w stosunku do skarg kierowanych przez osoby fizyczne przeciwko działalności administratora danych osobowych w danym państwie członkowskim.

The Regulation has established the European Data Protection Board ("EDPB") that takes over the responsibilities of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data. EDPB is an independent body of the European Union vested with legal personality. Its objective is to ensure consistent application of the provisions of the Regulation. At the national level, compliance with the new provisions is monitored by supervisory authorities. The new provisions establish the one-stop-shop rule, whereby in the event an enterprise processes personal data in more than one Member State, the competent supervisory authority for the enterprise's principal establishment is also competent for cross-border data processing and for all the obligations of that enterprise with regard to the implementation of the Regulation. The supervisory authorities of the individual Member States remain competent to handle complaints lodged by natural persons against the operations of a personal data controller in the relevant Member State.

W obecnym porządku prawnym funkcjonują zasady przetwarzania danych osobowych, jednakże w głównej mierze są to rekomendacje, nie zaś bezwzględnie obowiązujące przepisy prawa. Rozporządzenie wprowadza wprost zasady przetwarzania danych osobowych, a tym samym wiążące obowiązki dla podmiotów przetwarzających dane osobowe. Wprowadzenie katalogu podstawowych zasad ochrony danych osobowych stanowi podstawę nowych standardów ochrony danych oraz określa ramy dla pozostałych, szczegółowych przepisów Rozporządzenia.

While there are also personal data processing rules under the current legislation, these are mainly recommendations rather than mandatory provisions. The Regulation directly introduces personal data processing rules and thereby binding obligations applicable to personal data processors. The introduction of a list of fundamental personal data protection rules provides the basis for new standards of data protection as well as establishes a framework for the other specific provisions of the Regulation.

Mając na względzie doniosłość wprowadzanych zmian oraz dotkliwość ewentualnych sankcji nakładanych w związku z naruszaniem postanowień

Given the significance of the amendments and the severity of potential penalties imposed for infringements of the GDPR, this edition of the

RODO, niniejsze wydanie Polish Law Review zostało w całości poświęcone tematyce ochrony danych osobowych.

Polish Law Review is devoted in its entirety to the issues of personal data protection.

## POJĘCIE DANYCH OSOBOWYCH NA GRUNCIE RODO

## CONCEPT OF PERSONAL DATA UNDER GDPR

Nowe przepisy Rozporządzenia zastąpią zarówno dyrektywę regulującą materię ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodny przepływ takich danych, jak i będącą obecnie w mocy polską ustawę o ochronie danych osobowych. Wejście w życie Rozporządzenia oznacza szereg zmian, które dotkną przede wszystkim przedsiębiorców przetwarzających dane osobowe osób fizycznych, oferując towary lub usługi na terenie Unii Europejskiej.

The new provisions of the Regulation will replace both the directive governing the protection of individuals with regard to the processing of personal data and the free movement of such data and the currently effective Polish Act on Personal Data Protection. The Regulation's entry into force causes a number of changes that will mainly affect enterprises processing personal data of natural persons, offering goods or services in the European Union.

Jedną z najważniejszych nowości przewianych w Rozporządzeniu jest rozszerzenie definicji „danych osobowych". Celem tego rozszerzenia było dostosowanie pojęcia „danych osobowych" do praktyki obrotu gospodarczego, a w szczególności do przetwarzania danych w sieci. Pojęcie danych osobowych zostało w Rozporządzeniu zdefiniowane przez niewyczerpujące wyliczenie typów informacji o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

One of the most significant novelties of the Regulation is the expanded definition of "personal data". The purpose of the expansion was to realign the concept of personal data with business practice, and in particular with online data processing. The term personal data has been defined under the Regulation by way of non-exhaustive listing of the types of information relating to an identified or identifiable nature person.

Zgodnie z art. 4 pkt 1 Rozporządzenia, „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Rozporządzenie wskazuje, że możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Przywołane w przepisie kategorie danych to jedynie przykładowe wyliczenie, na co wskazuje zwrot „w szczególności". Samo Rozporządzenie wskazuje, że typem danych osobowych może być, np. identyfikator internetowy, czyli adres IP, identyfikator plików cookie lub inny identyfikator, generowany na przykład przez etykiety RFID albowiem taki identyfikator połączony z innym unikatowym identyfikatorem może być wykorzystany do stworzenia profilu lub zidentyfikowania danej osoby.

Pursuant to Article 4(1) of the Regulation, "personal data" means any information relating to an identified or identifiable natural person ('data subject'). The Regulation provides that an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The data categories referred to in the above provision are provided merely as examples, as indicated by the expression "in particular". As types of data, the Regulation itself lists for example online identifiers, i.e. IP addresses, cookie identifiers or other identifiers such as for instance radio frequency identification tags, as such identifiers when combined with another unique identifier may be used to create profiles of natural persons and identify them.

Rozporządzenie wyróżnia niektóre typy danych osobowych jako "szczególne kategorie danych

The Regulation distinguishes certain types of personal data as "special categories of personal

osobowych", których przetwarzanie, co do zasady, jest zabronione. Zgodnie z art. 9 ust. 1 Rozporządzenia w skład szczególnych kategorii danych osobowych wchodzą: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane dotyczące seksualności lub orientacji seksualnej danej osoby, dane genetyczne, dane biometryczne lub dane dotyczące zdrowia. Przepisy Rozporządzenia, precyzując te trzy ostatnie kategorie, wskazują np., że dane genetyczne dotyczą odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby. Dane biometryczne to dane dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, które umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Natomiast do danych dotyczących zdrowia należy zaliczyć wszelkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą, wyniki badań, numery identyfikacyjne, historie chorób, informacje o niepełnosprawności czy też informacje o leczeniu jakichkolwiek chorób.

data" whose processing is in principle prohibited. Pursuant to Article 9.1 of the Regulation special categories of personal data include: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and data concerning a natural person's sex life or sexual orientation, genetic data, biometric data, data concerning health. Provisions of the Regulation, by way of elaborating on the last three categories, stipulate for example that genetic data relates to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person. Biometric data means data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. In turn, data concerning health means all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject, examination results, identification numbers, medical histories, any information on disability or information on treatment of any diseases.

Należy uznać, że Rozporządzenie rozszerzyło znaczenie pojęcia „danych osobowych" poprzez dostosowanie go do wymogów obrotu e-commerce oraz powiązanych z tym metod identyfikacji jego uczestników, takich jak: numer IP, dane o geolokalizacji lub dane biometryczne.

In conclusion, the Regulation considerably extended the meaning of the term personal data by realigning it with the requirements of e-commerce and the related methods of identification of its participants, such as: IP address, geolocation, or biometric data.

## PRAWA I OBOWIĄZKI PRACODAWCÓW ZWIĄZANE Z RODO

Rozporządzenie będzie bezpośrednio stosowane w Polsce od dnia 25 maja 2018 roku. Z uwagi na konieczność dostosowania prawa krajowego do przepisów Rozporządzenia, polski ustawodawca pracuje nad projektem ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych (dalej jako „Projekt") – które przewidują dokonanie licznych zmian w wielu aktach prawnych, m.in. w kodeksie pracy. Projekt opracowywany jest przez Ministerstwo Cyfryzacji, obecnie na etapie opiniowania, przed końcem bieżącego roku przewiduje się jego przyjęcie przez Radę Ministrów. Poniżej przedstawiamy zarys obecnie planowanych w Projekcie rozwiązań w zakresie przetwarzania danych osobowych pracowników przez pracodawców z zaznaczeniem, że do czasu uchwalenia ustawy mogą one ulec zmianie.

## RIGHTS AND OBLIGATIONS OF EMPLOYERS UNDER GDPR

In Poland the direct application of the Regulation will take effect as of 25 May 2018. Given the necessary alignment of the national law with the Regulation, Polish legislators are working on a bill for Provisions Introducing the Act on Personal Data Protection ("Bill"), which proposes numerous amendments to many legislative acts, including the Labour Code. The Bill, which has been drafted by the Ministry of Digitisation and is currently at its opinion stage, is expected to be adopted by the Council of Ministers by the end of the current year. We outline below the solutions proposed under the Bill with regard to the processing by employers of the personal data of their employees, subject to any modifications and changes before the Bill is eventually enacted into law.

Projekt zakłada w szczególności dostosowanie brzmienia obowiązujących przepisów prawa pracy do wymogu zawartego w art. 6 ust. 1 lit. c Rozporządzenia, wprowadzającego przesłankę istnienia obowiązku prawnego jako podstawy pobierania danych osobowych. W konsekwencji przepisy, które obecnie zawierają jedynie uprawnienie pracodawcy żądania określonych danych osobowych w kwestiach związanych ze stosunkiem pracy, zostaną zmienione na obowiązek pobierania tych danych. Projekt przewiduje również modyfikację dotychczasowego katalogu danych osobowych pobieranych od kandydatów do pracy lub pracowników, uwzględniającą ich niezbędność dla pracodawcy, obligatoryjność ich pobierania oraz ochronę pracownika (zmiana art. $22^1$ k.p.). Między innymi pracodawcy mają mieć możliwość przetwarzania adresów poczty elektronicznej kandydatów do pracy i pracowników oraz ich numerów telefonu. Unormowane mają także zostać zasady wyrażenia zgody przez osobę ubiegającą się o zatrudnienie lub pracownika na pobranie określonych danych osobowych przez pracodawcę (np. pracodawca ma mieć możliwość przetwarzania danych biometrycznych pracowników w zakresie dotyczącym stosunku pracy, za ich zgodą). Dalej, ma zostać stworzony katalog danych, których pobieranie przez pracodawców ma być zabronione, nawet za zgodą osoby, której te dane dotyczą. Nowelizacja Kodeksu pracy ma także na celu uregulowanie prawne zasad stosowania przez pracodawców monitoringu, jako szczególnej formy przetwarzania danych osobowych. Monitoring ma być dopuszczalny dla zapewnienia bezpieczeństwa pracowników lub ochrony mienia albo zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Zabronione ma być natomiast stosowanie monitoringu w celu kontroli wykonywania pracy przez pracowników, jak również monitorowanie pomieszczeń niesłużących do wykonywania pracy, np. pomieszczeń sanitarnych, szatni, stołówek lub palarni. Do Projektu wprowadzono również podstawę prawną do pozyskiwania i przechowywania przez pracodawcę skierowań na badania lekarskie oraz orzeczeń lekarskich wydawanych w wyniku tego skierowania, jeżeli osoba przyjmowana do pracy u innego pracodawcy posiada aktualne orzeczenie lekarskie stwierdzające brak przeciwwskazań do pracy na danym stanowisku.

The Bill proposes in particular to realign the current provisions of the labour law with the requirement of Article 6.1(c) of the Regulation that introduces the condition of the existence of a legal obligation as the grounds for collecting personal data. Consequently, the regulations that currently provide only for the right of the employer to request specific personal data in matters relating to the employment relationship will be amended by imposing an obligation to collect such data. The Bill also envisages modification to the current list of personal data collected from job applicants or employees, taking into account its indispensability for the employer, mandatory nature of its collection, and protection of the employee (amendment to Article $22^1$ LC). Employers will be able, among others, to process email addresses of job applicants and employees as well as their telephone numbers. The rules for granting consent by a job applicant or an employee to the collection of his or her specific personal data by the employer (e.g. the employer will be able to process biometric data of its employees to the extent related to the employment relationship, subject to their consent) have also been established. Further, a list of data is to be provided, collection of which by employers will be prohibited, even with the consent of the data subject. Amendments to the Labour Code also seek to regulate the rules for application of monitoring by employers, as a special type of personal data processing. The use of monitoring will be permissible to safeguard employees or protect property or to ensure that information which disclosure could cause damage to the employer is kept confidential. On the other hand, the use of monitoring to check job performance of employees and to monitor facilities in which work is not performed, e.g. toilets, washrooms, and bathrooms, locker rooms, canteens, or smoking rooms, will be prohibited. The legal grounds for the collection and storing by the employer of referrals for medical examination and medical certificates issued as a result of such referrals, if a person being employed by a different employer holds an up-to-date medical certificate stating that there are no reasons to prevent him or her from working in the relevant position, have been also written into the Bill.

Poza Kodeksem pracy, Projekt przewiduje zmiany przepisów z sektora pracy zawartych także w następujących ustawach: o *ochronie roszczeń pracowniczych* w *razie niewypłacalności pracodawcy (ustawa* z dnia 13 lipca 2006 r.), o *szczególnych rozwiązaniach związanych* z *usuwaniem skutków powodzi (ustawa* z dnia 16

In addition to the Labour Code, the Bill also includes amendments to certain labour regulations laid down under the following statutes: Act on Protection of Workers' Claims in Case of Employer's Insolvency *of* 13 July 2006; *Act* on Special Arrangements for Remedying Flood Losses of 16 September 2011; Act on Special Arrangements for

września 2011 r.), o *szczególnych rozwiązaniach związanych* z *ochroną miejsc pracy (ustawa* z dnia 11 października 2013 r.).

Job Protection of 11 October 2013.

## ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH W ŚWIETLE RODO

Zarówno w obecnym stanie prawnym, jak i na gruncie Rozporządzenia, zgoda na przetwarzanie danych osobowych wyrażona przez osobę, której dane dotyczą, jest jedną z przesłanek legalizujących przetwarzanie danych osobowych. Jednak Rozporządzenie wprowadza istotne zmiany w zakresie pozyskiwania zgody na przetwarzanie danych osobowych. Wspomniane zmiany wymuszą wprowadzenie modyfikacji do procesu pozyskiwania zgody po 25 maja 2018 r., jak również mogą skutkować koniecznością ponownego pozyskania takiej zgody od osób, które zgody udzieliły na podstawie obecnie obowiązujących przepisów.

Na gruncie Rozporządzenia „zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Zatem podstawowymi przesłankami konstrukcyjnymi zgody są dobrowolność, konkretność, świadomość i jednoznaczność. Wyrażenie zgody powinno być oparte o zasadę opt-in, która wymaga od podmiotu danych podjęcia pozytywnego działania (np. zaznaczenia okienka zgody). Rozporządzenie wyklucza natomiast dopuszczalność modeli opt-out, które wykorzystują bierność lub milczenie, a często po prostu nieuwagę, osoby, której dane dotyczą (np. poprzez domyślne zaznaczenie okienka zgód).

Co istotne, Rozporządzenie uelastycznia podejście do wyrażania zgody względem obecnych regulacji, dopuszczając wyrażenie zgody nie tylko poprzez złożenie oświadczenia woli, ale także poprzez jej okazanie w inny sposób, np. poprzez wybór odpowiednich ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też inne zachowanie, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą zaakceptowała proponowane warunki przetwarzania jej danych osobowych. Złożenie oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych nie wymaga żadnej szczególnej formy. Jednak administrator danych musi być w stanie wykazać, że osoba, której dane dotyczą, taką zgodę wyraziła. Należy zatem wdrożyć odpowiednie środki organizacyjne i techniczne w zakresie utrwalania faktu wyrażenia zgody na przetwarzanie danych osobowych przez podmioty danych.

## CONSENT TO PROCESSING OF PERSONAL DATA UNDER GDPR

Both under the law as it stands now and under the Regulation, consent to the processing of personal data given by the data subject is one of the conditions that must be met to make processing of personal data lawful. However, the Regulation introduces significant changes in obtaining consent to personal data processing. The changes will make it necessary to modify the process of obtaining consent after May 25, 2018 and may require re-obtaining it from those who granted their consent under the regulations currently in force.

Under the Regulation, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wish by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Thus, the principal conditions of consent are that it must be freely given, specific, informed and unambiguous. Consent should be granted on an opt-in basis that requires some affirmative action (e.g. ticking the consent box) from the data subject. However, the Regulation excludes permissibility of opt-out arrangements that rely on inactivity or silence and often simply on inattentiveness of the data subject (e.g. pre-ticked consent boxes).

Importantly, compared to the current regime, the Regulation makes the approach to granting consent more flexible, by allowing it to be granted not only by making a declaration of intent but also in other ways, for example by choosing technical settings for information society services or another conduct that clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. The declaration of consent to the processing of personal data does not require to be made in any special form. However, the controller must be able to demonstrate that the data subject has granted his or her consent. Consequently, organisational and technical means must be put in place for recording the granting of consent by the data subject to the processing of his or her personal data.

Zgodnie z przepisami Rozporządzenia osoba, której dane dotyczą, ma prawo w dowolnym czasie wycofać zgodę na przetwarzanie danych osobowych. Co prawda powyższe uprawnienie występuje także na gruncie obecnych przepisów, jednak Rozporządzenie dodatkowo wymaga, aby w momencie zbierania danych osoba, której dane dotyczą, została o tym uprawnieniu poinformowana. Rozporządzenie wskazuje ponadto, że wycofanie zgody powinno być równie łatwe jak jej udzielenie. Administratorzy danych powinni zatem opracować procedury umożliwiające wycofanie zgody w sposób analogiczny do sposobu jej udzielenia.

Pursuant to the Regulation, the data subject is entitled to withdraw his or her consent to the processing of personal data at any time. While the above right is also present in the current regulations, the Regulation additionally requires that at the time personal data is obtained the data subject should be informed of the existence of the right to withdraw his or her consent. The Regulation further provides that withdrawal of consent should be as easy as giving consent. Thus, controllers should develop procedures for withdrawal of consent that correspond to the manner in which it is given.

Zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Rozporządzenie znacząco poszerza katalog informacji, jakie powinny być przekazane podmiotowi danych w momencie zbierania danych, m.in. wymagając wskazania okresu, przez jaki dane będą przechowywane, podanie informacji o prawie do cofnięcia zgody oraz informacji o zautomatyzowanym podejmowaniu decyzji. W związku z powyższym większość administratorów będzie musiała zaktualizować zakres informacji podawanych osobom, których dane dotyczą, w momencie zbierania danych.

The request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The Regulation extends significantly the list of information the data subject should be provided with at the time the data is obtained, including the time period over which the data is to be retained, the existence of the right to withdraw consent, and information on automated decision-making. In the light of the above, the majority of controllers will have to update the scope of information provided by them to data subjects at the time the data is obtained.

Jak wynika z powyższego, Rozporządzenie wprowadza wiele zmian w zakresie procesu pozyskiwania zgody na przetwarzanie danych osobowych. W związku ze zbliżającym się terminem stosowania Rozporządzenia (25 maja 2018 r.) przedsiębiorcy powinni zweryfikować czy mechanizmy, które stosują do pozyskiwania i przetwarzania danych są zgodne z nową regulacją i jakie niezbędne zmiany należałoby wprowadzić. Należy także przeanalizować, czy będzie można kontynuować przetwarzanie danych na podstawie zgody uzyskanej przed datą rozpoczęcia stosowania nowych regulacji. Zgodnie z motywem 171 preambuły Rozporządzenia, jeżeli przetwarzanie ma za podstawę zgodę w myśl obecnych przepisów, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, o ile pierwotny sposób jej wyrażenia odpowiada warunkom Rozporządzenia.

As indicated by the above, the Regulation introduces a number of changes in the process of obtaining consent to the processing of personal data. Given the imminent date on which the Regulation will become applicable (May 25, 2018), enterprises should check whether the mechanisms employed by them to obtaining and processing personal data are in line with the new provisions and what changes are necessary in that regard. They will also need to confirm whether they will be able to continue data processing under the consent given before the new provisions become applicable. According to recital 171 of the Regulation, where processing is based on consent given pursuant to the current provisions, it is not necessary for the data subject to give his or her consent again if the manner in which the consent was given complies with the conditions of the Regulation.

## PRAWO DO BYCIA ZAPOMNIANYM WEDŁUG RODO

## RIGHT TO BE FORGOTTEN UNDER GDPR

Rozporządzenie wprowadza między innymi prawo do usunięcia danych, zwane również „prawem do bycia zapomnianym". W teorii prawo to oznacza, że osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia

The Regulation introduces, among others, the right to erasure of personal data, also known as the "right to be forgotten". In theory, this means that the data subject has the right to request the controller to erase his or her personal data without

dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe w całości, jeżeli zachodzi jedna z wymienionych w Rozporządzeniu okoliczności. Administrator ma obowiązek usunąć dane osobowe na żądanie podmiotu danych osobowych, m.in., gdy:
- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opierało się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą wnosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych;
- dane zostały przetwarzane niezgodnie z prawem.

undue delay, and the controller has the obligation to erase all the personal data without undue delay if one of the grounds listed in the Regulation applies. The controller is required to erase personal data at the request of the data subject, among others, when:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;
- the data subject objects to the processing of his or her personal data;
- the personal data has been unlawfully processed.

Obowiązkiem wynikającym z Rozporządzenia, a ciążącym na administratorze jest także upewnienie się, że wszystkie kopie, repliki i inne odniesienia, (np. w postaci linków w Internecie) zostały usunięte. Nie wystarczy dezaktywacja danych, należy je całkowicie usunąć. Rozporządzenie obarcza administratora danych osobowych odpowiedzialnością za usunięcie treści przechowywanych przez osoby trzecie. Ciąży na nim również obowiązek poinformowania administratorów przetwarzających dane osobowe, że osoba, której dane dotyczą, żąda, aby jej dane osobowe zostały usunięte. Prawo do bycia zapomnianym ma szczególne znaczenie wtedy, gdy osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych, będąc dzieckiem, lub gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chciałaby usunąć dane osobowe jej dotyczące.

It is also the controller's obligation under the Regulation to ensure that all the copies, replications, or other references (e.g. online links to the data) are erased. It is not enough to merely deactivate the data, the data should be completely erased. The Regulation also makes the controller responsible for erasure of any data retained by third parties. The controller is also under an obligation to inform controllers processing personal data that the data subject has requested erasure of his or her personal data. The right to be forgotten is relevant in particular where the data subject has consented to the processing of his or her personal data as a child or was not fully aware of the risks involved by the processing and would subsequently wish to erase his or her personal data.

Rozporządzenie wprowadza także wyłączenia prawa do bycia zapomnianym. Prawo to nie ma zastosowania, w zakresie, w jakim przetwarzanie danych jest niezbędne:
- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- z uwagi na cele zdrowotne oraz interes publiczny w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
- do ustalenia, dochodzenia lub obrony roszczeń.

The Regulation also introduces exclusions from the right to be forgotten. The right does not apply to the extent that data processing is necessary:
- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by European Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- to safeguard the objectives of health and public interest in the area of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- for the establishment, exercise or defence of legal claims.

Administrator może odmówić usunięcia danych osobowych, powołując się na powyższe wyłączenia. W tej sytuacji brak usunięcia danych powinien być uznany za zgodny z prawem. Jednakże obowiązkiem administratora jest poinformowanie wnioskodawcy o przyczynach odmowy.

The controller may refuse to erase personal data on the grounds of the above exclusions. Under such circumstances, while failure to erase the data should be deemed lawful, it is the controller's obligation to inform the data subject of the reasons for the refusal.

Zmiana przepisów wiąże się z wieloma wyzwaniami dla administratorów danych osobowych oraz podmiotów, które przetwarzają dane na ich polecenie. Administratorzy będą zmuszeni, pod rygorem narażenia się na odpowiedzialność finansową, do dostosowania wewnętrznych procedur do celów realizacji praw podmiotów danych osobowych. Najwięcej problemów może przysporzyć zapewnienie szybkiej i efektywnej odpowiedzi na żądanie usunięcia danych osobowych. Wiele podmiotów przechowuje ogromną ilość danych osobowych. Organizacyjne i techniczne przeszkody mogą zatem w znacznym stopniu utrudnić realizację dużej ilości żądań w krótkim czasie. W praktyce wyegzekwowanie skuteczności wniosku o usunięciu danych osobowych może okazać się niezwykle trudne.

The amendment of the law poses many challenges to controllers of personal data and processors that process the data at controllers' request. Under pain of financial liability, controllers will need to realign their internal procedures with the purposes of protection of the rights vested in data subjects. Ensuring a fast and effective response to the request for erasure of personal data can become the main issue. Many enterprises retain massive amounts of personal data. Thus, organisational and technical obstacles can prove a material hindrance to the processing of a large number of such requests in a short period of time. In practice, enforcing the effectiveness of a request for erasure of personal data may prove very difficult indeed.

## ANALIZA RYZYKA NA GRUNCIE RODO

## IMPACT ASSESSMENT UNDER GDPR

Kolejną nowość wprowadzaną przez Rozporządzenie stanowi obowiązek przeprowadzenia przez administratora danych analizy ryzyka. Wymuszenie takiej analizy, poprzez ustanowienie jej jednym z podstawowych obowiązków administratora danych w określonych przez Rozporządzenie sytuacjach, ma na celu zwiększenie świadomości niebezpieczeństw występujących przy przetwarzaniu danych osobowych. Ewentualny wyciek danych osobowych może, bowiem spowodować znacznie większe straty niż jedynie koszt odszkodowań.

Another novelty ushered in by the Regulation is the controller's obligation to carry out an impact assessment. Imposition of the assessment, as made one of the principal obligations of the controller in the circumstances identified under the Regulation, seeks to improve the awareness of risks attendant upon the processing of personal data. As it happens, a personal data breach may cause much more damage than the cost of compensation alone.

W praktyce przeprowadzenie analizy ryzyka związanego z przetwarzaniem danych osobowych powinno nastąpić przed rozpoczęciem przetwarzania danych przez administratora. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych - przeprowadzenie analizy ryzyka jest obligatoryjne. Zgodnie z Rozporządzeniem, przeprowadzając analizę, administrator danych konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony. Ocena skutków dla ochrony danych jest w szczególności wymagana w przypadku:

In practice, an assessment of the impact upon personal data processing should precede processing of such data by the controller. If the relevant type of processing, in particular using new technologies, is highly likely, taking into account its nature, scope, context, and purposes, to result in a high risk of infringing the rights or freedoms of natural persons, an impact assessment is mandatory. Pursuant to the Regulation, when carrying out the assessment, the controller seeks the advice of the data protection officer, where designated. A data protection impact assessment is in particular required in the case of:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa; lub

b) processing on a large scale of special categories of personal data or of personal data relating to criminal convictions and offences; or

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

c) a systematic monitoring of publicly accessible areas on a large scale.

Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych oraz przekazuje te wykazy Europejskiej Radzie Ochrony Danych.

The supervisory authority establishes and makes public a list of the types of processing operations which are subject to the requirement for a data protection impact assessment and communicates the list to the European Data Protection Board.

Ocena skutków dla ochrony danych będąca wynikiem wykonanej analizy ryzyka powinna zawierać co najmniej:

A data protection impact assessment should contain at least:

- opis planowanych operacji przetwarzania i celów przetwarzania;
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie przepisów Rozporządzenia.

- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of the data subjects;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation.

Jeżeli ocena skutków dla ochrony danych wykaże, że przetwarzanie mogłoby spowodować wysokie ryzyko, w przypadku nie zastosowania przez administratora środków mających na celu zminimalizowanie tego ryzyka, to, zgodnie z Rozporządzeniem, przed rozpoczęciem przetwarzania konieczne będzie zasięgnięcie konsultacji organu nadzorczego. Jeśli zaś organ nadzorczy stwierdzi, że zamierzone przetwarzanie danych stanowiłoby naruszenie Rozporządzenia – w szczególności, gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – to organ nadzorczy udzieli administratorowi pisemnych zaleceń oraz będzie mógł skorzystać z uprawnień przysługujących mu na podstawie przepisów Rozporządzenia. Co do zasady, takie konsultacje będą trwały osiem tygodni. Termin ten może jednak ulec przedłużeniu, ponadto bieg tego terminu można zawiesić do czasu, aż organ

If a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate it, then pursuant to the Regulation, the controller must consult the supervisory authority prior to processing. Where the supervisory authority is of the opinion that the intended processing would infringe the Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority provides written advice to the controller and may use any of its powers conferred by the Regulation. In principle, the consultations last eight weeks. That period may be extended or suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

nadzorczy uzyska wszelkie informacje, których zażądał dla celów konsultacji.

## NARUSZENIE PRZEPISÓW ZAWARTYCH W RODO ORAZ ZWIĄZANE Z TYM REPERKUSJE FINANSOWE

W związku z wejściem w życie przepisów Rozporządzenia, GIODO będzie posiadał uprawnienie do nakładania administracyjnych kar pieniężnych, w wysokości zależnej od danego naruszenia. Kary mają być w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające. Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku. Ustalając ich wysokość, bierze się pod uwagę m.in.:

1. charakter, wagę i czas trwania naruszenia;
2. umyślny lub nieumyślny charakter naruszenia;
3. działania podjęte przez administratora lub podmiot przetwarzający;
4. stopień odpowiedzialności administratora lub podmiotu przetwarzającego;
5. wcześniejsze naruszenia; oraz
6. kategorie danych osobowych, których dotyczyło naruszenie.

Jeżeli administrator lub podmiot przetwarzający dane osobowe narusza w ramach tych samych lub powiązanych czynności kilka przepisów Rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie może przekroczyć wysokości kary za najpoważniejsze naruszenie.

Wysokość kary administracyjnej zależy od tego, jakie naruszenie zostało popełnione. Rozporządzenie dzieli naruszenia na dwie kategorie. Pierwsza dotyczy podstawowych zasad przetwarzania danych. Naruszenia tych przepisów zagrożone są administracyjną karą pieniężną w wysokości do 20 000 000 euro a w przypadku przedsiębiorstwa w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Drugą kategorią są naruszenia obowiązków administratora i podmiotu przetwarzającego dane osobowe, które zostały wymienione w katalogu zamkniętym w art. 83 ust. 4 Rozporządzenia. Naruszenia te zagrożone są administracyjną karą pieniężną w wysokości do 10 000 000 euro a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego

## INFRINGEMENT OF GDPR AND RELATED FINANCIAL RAMIFICATIONS

With the effectiveness of the Regulation, the Inspector General for Protection of Personal Data ("GIODO") is given the power to impose administrative fines in an amount commensurate with the severity of a specific infringement. The fines imposed in each individual case must be effective, proportionate and dissuasive. Administrative fines are imposed depending on the circumstances of each individual case. When deciding on the amount of the administrative fine, due regard is given, among others, to the following:

1. the nature, gravity and duration of the infringement;
2. the intentional or negligent character of the infringement;
3. any action taken by the controller or processor;
4. the degree of responsibility of the controller or processor;
5. previous infringements; and
6. the categories of personal data affected by the infringement.

If a controller or processor infringes several provisions of the Regulation, for the same or linked processing operations, the total amount of the administrative fine cannot exceed the amount specified for the gravest infringement.

The amount of the administrative fine depends on what infringement has been committed. The Regulation differentiates between two categories of infringements. The first one comprises infringements of the fundamental rules of data processing. These infringements are subject to an administrative fine of up to EUR 20,000,000, or in the case of an undertaking, of up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher. The other category includes infringements of the obligations of the controller and the processor comprised in the exhaustive list of Article 83.4 of the Regulation. These infringements are subject to an administrative fine of up to EUR 10,000,000, or in the case of an undertaking, of up to 2% of its total worldwide annual turnover of the preceding financial year, whichever is higher. The fine

światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Wysokości kar zostały obniżone dla podmiotów publicznych, o których mowa w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 roku o finansach publicznych - do wysokości 100 000 złotych.

amounts have been reduced to PLN 100,000 for the public entities referred to under Article 9(1)-(12) and (14) of the Public Finance Act of 27 August 2009.

Równowartość powyżej wskazanych kwot, które zostały wyrażone w euro, będzie obliczana w polskich złotych według średniego kursu euro ogłoszonego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku.

The PLN equivalent of the above amounts expressed in EUR is calculated at the average EUR exchange rate published by the National Bank of Poland in the table of average exchange rates as at 28 January of each year.

Warto również wspomnieć, że każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia Rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego dane osobowe odszkodowanie za poniesioną szkodę. Odszkodowania tego może domagać się na drodze sądowej.

It is also worth noting that any person who has suffered material or non-material damage as a result of an infringement of the Regulation has the right to receive compensation from the controller or processor for the damage suffered. The right to receive the compensation referred to above is exercised under court proceedings.

Biorąc pod uwagę wysokość grożących kar, podmioty przetwarzające dane osobowe powinny już teraz zainteresować się wdrożeniem nowych rozwiązań gwarantujących przestrzeganie przepisów Rozporządzenia.

Given the high rates of fines that can be imposed, it is by no means too early for processors to take an interest in putting in place new arrangements to ensure compliance with the Regulation.

## TRANSFER DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

## TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Rozporządzenie określa zasady przekazywania danych osobowych, które następnie są lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej. Zgodnie z ogólną zasadą przekazanie może nastąpić tylko wtedy, gdy administrator i podmiot przetwarzający spełniają wymogi dotyczące przekazywania danych osobowych określone w Rozporządzeniu, włącznie z wymogami dalszego przekazania danych.

The Regulation lays down the principles for transfer of personal data that is undergoing processing or is intended for processing after transfer to a third country or to an international organisation. The general principle for the transfers is that any transfer may take place only if the conditions for personal data transfer set forth under the Regulation, including with respect to onward transfers of personal data, are complied with by the controller and processor.

Transfer danych osobowych jest możliwy, jeżeli państwo trzecie lub organizacja międzynarodowa zapewnia adekwatny poziom ochrony danych osobowych. Podobne regulacje obowiązywały na podstawie Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dalej jako „Dyrektywa"). Adekwatność poziomu ochrony danych osobowych może zostać zatwierdzona decyzją Komisji Europejskiej. Dotychczas wydane decyzje dotyczące adekwatności zostają utrzymane w mocy bezterminowo, do czasu ich uchylenia lub zmiany. Obecnie funkcjonujące decyzje Komisji Europejskiej dotyczą: Andory, Argentyny, Kanady,

A transfer of personal data may take place if the third country or the international organisation in question ensures an adequate level of protection with respect to personal data. Similar provisions were in place under Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter as "Directive"). The adequacy of the level of protection with respect to personal data can be approved under a decision adopted by the European Commission. The adequacy decisions that have been adopted remain in force for an indefinite period until repealed or amended. The currently effective decisions of the European Commission pertain to: Andorra,

Szwajcarii, Izraela, wysp Guernsey, Jersey, Man, Nowej Zelandii, Urugwaju oraz szczególnego uregulowania transferu danych pomiędzy obszarem Unii Europejskiej a Stanami Zjednoczonymi – Privacy Shield.

Privacy Shield stanowi nowy pakiet przepisów dotyczących przekazywania danych osobowych pomiędzy Unią Europejską a Stanami Zjednoczonymi, który zastąpił poprzedni - Safe Harbour. Zgodnie z decyzją Privacy Shield, podmioty ze Stanów Zjednoczonych chcące przetwarzać dane osobowe przekazywane z Unii Europejskiej muszą przestrzegać zasad, które zapewniają ochronę prywatności osób fizycznych. Jedną z podstawowych zasad stanowi prawo do informacji. Osoby fizyczne muszą być informowane, m.in. o rodzaju przetwarzanych danych, celu ich przetwarzania czy prawie dostępu do danych. Podmioty przetwarzające dane są też zobowiązane do publikowania swoich polityk prywatności.

Przekazywanie danych osobowych jest również możliwe w razie braku decyzji Komisji Europejskiej. W takim przypadku jednak administrator lub podmiot przetwarzający mogą przekazać dane osobowe wyłącznie wtedy, gdy zapewnią odpowiednie zabezpieczenia, oraz pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Odpowiednie gwarancje można zapewnić m.in. za pomocą prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi czy wiążących reguł korporacyjnych. Ponadto, zgodnie z Rozporządzeniem, przekazanie danych osobowych do państwa trzeciego jest możliwe także wtedy, gdy brak jest decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń. W takim przypadku przekazanie danych możliwe jest wyłącznie pod warunkiem wystąpienia jednego z wymienionych w Rozporządzeniu wyjątków mających zastosowanie w szczególnych sytuacjach. Rozporządzenie poszerza katalog wyjątków. Wszystkie odstępstwa od zakazu transferu danych osobowych zawarte w Dyrektywie pozostają w mocy. Dodatkowo przekazanie danych będzie możliwe także wtedy, gdy jest ono niezbędne do zawarcia umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą; gdy przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; a także, gdy przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń.

Argentina, Canada, Switzerland, Israel, the islands of Guernsey, Jersey, Isle of Man, New Zealand, Uruguay, and to the special regulations governing transfer of data between the European Union and the US – the Privacy Shield.

The Privacy Shield is a new package of legislation governing the transfer of personal data between the European Union and the US that replaced the previous one – the Safe Harbour. Under the Privacy Shield decision, US processors wishing to process personal data transferred from the European Union must comply with the principles ensuring protection of the privacy of individuals. The right to information is one of the fundamental principles. Individuals must be informed, among others, of the type of data processed, purpose of the processing, or the right of access to the data. Processors are also required to publish their privacy policies.

A transfer of personal data may also take place in the absence of a decision of the European Commission. However, under such circumstances a controller or processor may transfer personal data only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards may be provided for, among others, by a legally binding and enforceable instrument between public authorities or bodies or binding corporate rules. Further, pursuant to the Regulation, a transfer of personal data to a third country may also take place in the absence of an adequacy decision or appropriate safeguards. Under such circumstances, a transfer of data may take place only if one of the derogations for special situations listed under the Regulation occurs. The Regulation extends the list of the derogations. All the derogations from prohibition on transfer of personal data set forth under the Directive remain in force. Additionally, a transfer of data may take place if it is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; if the transfer is necessary in order to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent; and when the transfer is necessary for the establishment, exercise or defence of legal claims.

*Pod redakcją / Supervising Editors: Małgorzata Fituch i Grzegorz Żebrowski*


**MILLER, CANFIELD,**
**W. BABICKI, A. CHEŁCHOWSKI I WSPÓLNICY SP.K.**

ul. Batorego 28-32
81-366 **Gdynia**
Tel. +48 58 782-0050
Fax +48 58 782-0060
gdynia@pl.millercanfield.com

ul. Nowogrodzka 11
00-513 **Warszawa**
Tel. +48 22 447-4300
Fax +48 22 447-4301
warszawa@pl.millercanfield.com

ul. Skarbowców 23a
53-125 **Wrocław**
Tel. +48 71 780-3100
Fax +48 71 780-3101
wroclaw@pl.millercanfield.com

**millercanfield.pl**

POLAND * USA * CANADA * MEXICO * CHINA